PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 14 May 1998 (14.05.98)	
International application No. PCT/EP97/05081	**Applicant's or agent's file reference** P96029WO/EK16-5
International filing date (day/month/year) 17 September 1997 (17.09.97)	**Priority date** (day/month/year) 01 October 1996 (01.10.96)
Applicant SCHEERHORN, Alfred et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

23 April 1998 (23.04.98)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Ingrid Hours

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

09/369830

PCT

From the INTERNATIONAL BUREAU

To:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

NOTIFICATION CONCERNING DOCUMENT TRANSMITTED

Date of mailing (day/month/year) 07 April 1999 (07.04.99)	
International application No. PCT/EP97/05081	**International filing date** (day/month/year) 17 September 1997 (17.09.97)
Applicant DEUTSCHE TELECOM AG et al	

The International Bureau transmits herewith the following documents and number thereof:

_____ copy of the English translation of the international preliminary examination report (Article 36(3)(a))

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

A. Karkachi

Telephone No.: (41-22) 338.83.38

Copy for the Elected Office (EO/US) PCT/EP97/05081

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

DEUTSCHE TELEKOM AG
Technologiezentrum
Patentabteilung EK03
D-64307 Darmstadt
ALLEMAGNE

Date of mailing (day/month/year) 14 May 1998 (14.05.98)	
Applicant's or agent's file reference P96029WO/EK16-5	**IMPORTANT NOTIFICATION**
International application No. PCT/EP97/05081	**International filing date** (day/month/year) 17 September 1997 (17.09.97)

1. The following indications appeared on record concerning:

[X] the applicant [ ] the inventor [ ] the agent [ ] the common representative

Name and Address	State of Nationality	State of Residence
DEUTSCHE TELEKOM AG Technologiezentrum, EK16-5 Postfach 10 00 03 D-64276 Darmstadt Germany	DE	DE
	Telephone No. +49 (61 51) 83-58 46	
	Facsimile No. +49 (61 51) 83-58 43	
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address	State of Nationality	State of Residence
DEUTSCHE TELEKOM AG Technologiezentrum Patentabteilung EK03 D-64307 Darmstadt Germany	DE	DE
	Telephone No. +49 (61 51) 83-58 46	
	Facsimile No. +49 (61 51) 83-58 43	
	Teleprinter No.	

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[X] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Ingrid Hours
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

Form PCT/IB/306 (March 1994) 002039712

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
P96029WO/EK16-5		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/EP 97/05081	17/09/1997	01/10/1996
Anmelder		
DEUTSCHE TELECOM AG et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. [ ] **Bestimmte Ansprüche haben sich als nichtrecherchierbar erwiesen** (siehe Feld I).

2. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

3. [ ] In der internationalen Anmeldung ist **ein Protokoll einer Nucleotid- und/oderAminosäuresequenz** offenbart; die internationale Recherche wurde auf der Grundlage des Sequenzprotokolls durchgeführt,
   - [ ] das zusammen mit der internationalen Anmeldung eingereicht wurde.
   - [ ] das vom Anmelder getrennt von der internationalen Anmeldung vorgelegt wurde,
     - [ ] dem jedoch keine Erklärung beigefügt war, daß der Inhalt des Protokolls nicht über den Offenbarungsgehalt der internationalen Anmeldung in der eingereichten Fassung hinausgeht.
   - [ ] das von der Internationalen Recherchenbehörde in die ordnungsgemäße Form übertragen wurde.

4. Hinsichtlich der **Bezeichnung der Erfindung**
   - [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.
   - [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt.

5. Hinsichtlich der **Zusammenfassung**
   - [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.
   - [ ] wurde der Wortlaut nach Regel 38.2b) in der Feld III angegebenen Fassung von dieser Behörde festgesetzt. Der Anmelder kann der Internationalen Recherchenbehörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen:
   Abb. Nr. 1
   - [X] wie vom Anmelder vorgeschlagen
   - [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.
   - [ ] weil diese Abbildung die Erfindung besser kennzeichnet.
   - [ ] keine der Abb.

INTERNATIONAL SEARCH REPORT

Intern. nal Application No
PCT/EP 97/05081

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimumdocumentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 94 21066 A (TELSTRA) 15 September 1994 see page 4, line 6 - line 15 see page 6, line 10 - line 17 see page 7, line 17 - page 8, line 3	1,2
A	JUENEMAN ET AL.: "MESSAGE AUTHENTICATION WITH MANIPULATION DETECTION CODES" PROCEEDINGS OF THE 1983 SYMPOSIUM ON SECURITY AND PRIVACY, 25 April 1983, SILVER SPRING (US), pages 33-54, XP002055686 see page 33, right-hand column, paragraph 4 see page 41, left-hand column, line 29 - right-hand column, line 30 see page 42, left-hand column, line 7 - line 12	1

[ ] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publicationdate of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of theinternational search	Date of mailing of the international search report
13 February 1998	27/02/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

EL696149475

INTERNATIONAL SEARCH REPORT

information on patent family members

Intern nal Application No
PCT/EP 97/05081

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9421066 A	15-09-94	AU 683646 B	20-11-97
		AU 6255694 A	26-09-94

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P96029WO/EK03-3	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP97/05081	International filing date (*day/month/year*) 17 September 1997 (17.09.1997)	Priority date (*day/month/year*) 01 October 1996 (01.10.1996)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant DEUTSCHE TELECOM AG		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 10 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
23 April 1998 (23.04.1998)	23 February 1999 (23.02.1999)
Name and mailing address of the IPEA/EP European Patent Office D-80298 Munich, Germany Facsimile No. 49-89-2399-4465	Authorized officer Telephone No. 49-89-2399-0

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP97/05081

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1,5,7,9, as originally filed,
pages _____, filed with the demand,
pages 2-4,6,8, filed with the letter of 22 September 1998 (22.09.1998),
pages _____, filed with the letter of _____.

☒ the claims, Nos. 3,4,6,7,10, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1,2,5,8,9, filed with the letter of 22 September 1998 (22.09.1998),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/2,2/2, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1 - 10	YES
	Claims		NO
Inventive step (IS)	Claims	1 - 10	YES
	Claims		NO
Industrial applicability (IA)	Claims	1 - 10	YES
	Claims		NO

2. Citations and explanations

1. Prior art

The invention concerns a method of transmitting signal/data sequences between a transmitter and a receiver with authentication of the transmitted signal/data sequences by using codes and cryptographic algorithms which are implemented at both the transmitter and at the receiver end.

Authenticated transmission of data or signals plays an increasingly important role in the transmission of signal sequences; for example, "ISO/IEC 9797, Information Technology - Security techniques - Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm" (JTC1/SC27 1994) describes one solution to this problem.

However, the **disadvantage** of this solution is that the checksum of a signal has to be calculated as a function of the checksum of the previously transmitted signals in order to detect a change in the sequence of the transmitted data. This is necessary even when a checksum is sent after every

signal, since otherwise an attacker could record pairs of signal checksums and alter their sequence in undetected manner. With the known solution, this requires the cryptographic algorithm to be carried out for each checksum. Since the sequence and choice of signals are not set precisely in advance, it is also impossible to calculate the necessary checksums in advance. This can be problematic in a time-critical environment.

2. Problem, solution and its advantages

Consequently, the **problem** addressed by the invention is to devise a method of authenticated signal or data transmission which enables authentication information to be calculated in advance for a predetermined signal set and a predetermined maximum number of signals to be transmitted, such that, in the communication phase, checksums for the transmitted signals or data can be calculated rapidly and simply from this already calculated information.

According to the invention, the **solution** to this problem is that, in a pre-calculation phase, cryptographic algorithms are used to calculate data as a function of a secret code and, in a subsequent communication phase, authentication tokens authenticating both the signals and the sequence in which they are transmitted are calculated from those data.

The **advantage** of this solution is that, owing to the deliberate introduction of a pre-calculation phase and a communication phase into the transmission

process, it is now possible to calculate authentication data before the actual communication phase. During the transmission phase, checksums for the transmitted signals can now be calculated simply and rapidly from these previously calculated data.

The claimed concept is also neither disclosed nor suggested by the two "A" category documents cited in the international search report, which are more remote from the subject matter of Claim 1 than the above-mentioned prior art.

The subject matter of Claim 1 obviously also has industrial applicability.

Therefore the present Claim 1 satisfies the novelty, inventive step and industrial applicability requirements of PCT Article 33(1) to (4).

Claims 2 to 10 are dependent on Claim 1 and so can also be considered novel, inventive and industrially applicable.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. On page 3, line 7, of the description the word "**are**" should be changed to "**is**" since grammatically the sentence should correctly read: "In the precalculation phase *a pseudo random sequence Z is generated* …".

2. In Claim 9 "**according to the preamble of Claim 1 or**" should have been deleted. Since the applicants agreed to delete this phrase, it was presumably left in by oversight.

Einschreiben an EPA München

PCT

Vertrag + Text (3fach)
Gebührenblatt
Antrag
Probelag

ANTRAG

Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird.

Vom Anmeldeamt auszufüllen

Internationales Aktenzeichen — Gef. Rdl 12/9

Internationales Anmeldedatum — Vgl. — Abges. A Upl 12/09. — Anl.

Name des Anmeldeamts und "PCT International Application".

Aktenzeichen des Anmelders oder Anwalts *(falls gewünscht)* *(max. 12 Zeichen)* P96029WO/EK16-5

Feld Nr. I BEZEICHNUNG DER ERFINDUNG

Verfahren zur Übertragung von Signalen

Feld Nr. II ANMELDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)*

Deutsche Telekom AG

Friedrich-Ebert-Allee 140

D - 53113 Bonn

Deutschland

☐ Diese Person ist gleichzeitig Erfinder

Telefonnr.:

Telefaxnr.:

Fernschreibnr.:

Staatsangehörigkeit (Staat): DE

Sitz oder Wohnsitz (Staat): DE

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☒ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben)*

Dr. Scheerhorn, Alfred
Ahornallee 3
D - 49716 Meppen

Deutschland

Diese Person ist

☐ nur Anmelder

☒ Anmelder und Erfinder

☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat): DE

Sitz oder Wohnsitz (Staat): DE

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☒ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

☒ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem Fortsetzungsblatt angegeben.

Feld Nr. IV ANWALT ODER GEMEINSAMER VERTRETER; ZUSTELLANSCHRIFT

Die folgende Person wird hiermit bestellt/ist bestellt worden, um für den (die) Anmelder vor den zuständigen internationalen Behörden in folgender Eigenschaft zu handeln als: ☐ Anwalt ☐ gemeinsamer Vertreter

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)*

Deutsche Telekom AG
Technologiezentrum, EK16-5
Postfach 10 00 03
D - 64276 Darmstadt
Deutschland

Telefonnr.: + 49 (61 51) 83-58 46

Telefaxnr.: + 49 (61 51) 83-58 43

Fernschreibnr.:

☒ Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und statt dessen im obigen Feld eine spezielle Zustellanschrift angegeben ist.

Fortsetzung von Feld Nr. III **WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER**

Wird keines der folgenden Felder benutzt, so ist dieses Blatt dem Antrag nicht beizufügen.

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben)*

Dr. Huber, Klaus
Ernst-Ludwig-Str. 21
D - 64283 Darmstadt

Deutschland

Diese Person ist:
☐ nur Anmelder
☒ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat): DE
Sitz oder Wohnsitz (Staat): DE

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☒ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben)*

Diese Person ist:
☐ nur Anmelder
☐ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat):
Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben)*

Diese Person ist:
☐ nur Anmelder
☐ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat):
Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben)*

Diese Person ist:
☐ nur Anmelder
☐ Anmelder und Erfinder
☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat):
Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

☐ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem zusätzlichen Fortsetzungsblatt angegeben.

Formblatt PCT/RO/101 (Fortsetzungsblatt) (Juli 1993; Nachdruck Januar 1996) *Siehe Anmerkungen zu diesem Antragsformular*

Feld Nr. V BESTIMMUNG VON STAATEN

Die folgenden Bestimmungen nach Regel 4.9 Absatz a werden hiermit vorgenommen *(bitte die entsprechenden Kästchen ankreuzen: wenigstens ein Kästchen muß angekreuzt werden)*:

Regionales Patent

☐ AP **ARIPO-Patent:** GH Ghana, KE Kenia, LS Lesotho, MW Malawi, SD Sudan, SZ Swasiland, UG Uganda, ZW Simbabwe und jeder weitere Staat, der Vertragsstaat des Harare-Protokolls und des PCT ist

☐ EA **Eurasisches Patent:** AM Armenien, AZ Aserbaidschan, BY Belarus, KG Kirgisistan, KZ Kasachstan, MD Republik Moldau, RU Russische Föderation, TJ Tadschikistan, TM Turkmenistan und jeder weitere Staat, der Vertragsstaat des Eurasischen Patentübereinkommens und des PCT ist

☒ EP **Europäisches Patent:** AT Österreich, BE Belgien, CH und LI Schweiz und Liechtenstein, DE Deutschland, DK Dänemark, ES Spanien, FI Finland, FR Frankreich, GB Vereinigtes Königreich, GR Griechenland, IE Irland, IT Italien, LU Luxemburg, MC Monaco, NL Niederlande, PT Portugal, SE Schweden und jeder weitere Staat, der Vertragsstaat des Europäischen Patentübereinkommens und des PCT ist

☐ OA **OAPI-Patent:** BF Burkina Faso, BJ Benin, CF Zentralafrikanische Republik, CG Kongo, CI Côte d'Ivoire, CM Kamerun, GA Gabun, GN Guinea, ML Mali, MR Mauretanien, NE Niger, SN Senegal, TD Tschad, TG Togo und jeder weitere Staat, der Vertragsstaat der OAPI und des PCT ist *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)* .....

Nationales Patent *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)*:

☐ AL Albanien
☐ AM Armenien
☐ AT Österreich
☐ AU Australien
☐ AZ Aserbaidschan
☐ BA Bosnien-Herzegowina
☐ BB Barbados
☐ BG Bulgarien
☐ BR Brasilien
☐ BY Belarus
☒ CA Kanada
☐ CH und LI Schweiz und Liechtenstein
☐ CN China
☐ CU Kuba
☐ CZ Tschechische Republik
☐ DE Deutschland
☐ DK Dänemark
☐ EE Estland
☐ ES Spanien
☐ FI Finnland
☐ GB Vereinigtes Königreich
☐ GE Georgien
☐ GH Ghana
☐ HU Ungarn
☒ IL Israel
☐ IS Island
☒ JP Japan
☐ KE Kenia
☐ KG Kirgisistan
☐ KP Demokratische Volksrepublik Korea
☐ KR Republik Korea
☐ KZ Kasachstan
☐ LC Saint Lucia
☐ LK Sri Lanka
☐ LR Liberia
☐ LS Lesotho
☐ LT Litauen
☐ LU Luxemburg
☐ LV Lettland
☐ MD Republik Moldau
☐ MG Madagaskar
☐ MK Die ehemalige jugoslawische Republik Mazedonien
☐ MN Mongolei
☐ MW Malawi
☐ MX Mexiko
☐ NO Norwegen
☐ NZ Neuseeland
☐ PL Polen
☐ PT Portugal
☐ RO Rumänien
☐ RU Russische Föderation
☐ SD Sudan
☐ SE Schweden
☐ SG Singapur
☐ SI Slowenien
☐ SK Slowakei
☐ SL Sierra Leone
☐ TJ Tadschikistan
☐ TM Turkmenistan
☐ TR Türkei
☐ TT Trinidad und Tobago
☐ UA Ukraine
☐ UG Uganda
☒ US Vereinigte Staaten von Amerika
☐ UZ Usbekistan
☐ VN Vietnam
☐ YU Jugoslawien
☐ ZW Simbabwe

Kästchen für die Bestimmung von Staaten (für die Zwecke eines nationalen Patents), die dem PCT nach der Veröffentlichung dieses Formblatts beigetreten sind:

☐ .....
☐ .....
☐ .....
☐ .....
☐ .....

Zusätzlich zu den oben genannten Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der Bestimmung von _____

Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt. *(Die Bestätigung einer Bestimmung erfolgt durch die Einreichung einer Mitteilung, in der diese Bestimmung angegeben wird, und die Zahlung der Bestimmungs- und der Bestätigungsgebühr. Die Bestätigung muß beim Anmeldeamt innerhalb der Frist von 15 Monaten eingehen.)*

Siehe Anmerkungen zu diesem Antragsformular

Feld Nr. VI PRIORITÄTSANSPRUCH Weitere Prioritätsansprüche sind im Zusatzfeld angegeben. ☐

Die Priorität der folgenden früheren Anmeldung(en) wird hiermit beansprucht:

Staat (Anmelde- oder Bestimmungsstaat der Anmeldung)	Anmeldedatum (Tag/Monat/Jahr)	Aktenzeichen	Anmeldeamt (nur bei regionaler oder internationaler Anmeldung)
(1) DE	01. Oktober 1996 (01.10.96)	196 40 526.2	
(2)			
(3)			

Dieses Kästchen ankreuzen, wenn die beglaubigte Kopie der früheren Anmeldung von dem Amt ausgestellt werden soll, das für die Zwecke dieser internationalen Anmeldung Anmeldeamt ist (eine Gebühr kann verlangt werden):

☐ Das Anmeldeamt wird hiermit ersucht, eine beglaubigte Abschrift der oben in Zeile(n) _____ bezeichneten früheren Anmeldung(en) zu erstellen und dem Internationalen Büro zu übermitteln.

Feld Nr. VII INTERNATIONALE RECHERCHENBEHÖRDE

Wahl der Internationalen Recherchenbehörde (ISA) *(Sind zwei oder mehr Internationale Recherchenbehörden für die internationale Recherche zuständig, ist der Name der Behörde anzugeben, die die internationale Recherche durchführen soll; Zweibuchstaben-Code genügt):* ISA/ _____

Frühere Recherche: *Auszufüllen, wenn eine Recherche (internationale Recherche, Recherche internationaler Art oder sonstige Recherche) bereits bei der internationalen Recherchenbehörde beantragt oder von ihr durchgeführt worden ist und diese Behörde nun ersucht wird, die internationale Recherche soweit wie möglich auf die Ergebnisse einer solchen früheren Recherche zu stützen. Die Recherche oder der Recherchenantrag ist durch Angabe der betreffenden Anmeldung (bzw. deren Übersetzung) oder des Recherchenantrags zu bezeichnen.*

Staat (oder regionales Amt): Datum *(Tag/Monat/Jahr)*: Aktenzeichen:

Feld Nr. VIII KONTROLLISTE

Diese internationale Anmeldung umfaßt:

1. Antrag	: 5	Blätter
2. Beschreibung	: 9	Blätter
3. Ansprüche	: 3	Blätter
4. Zusammenfassung	: 1	Blätter
5. Zeichnungen:	2	Blätter
Insgesamt	: 20	Blätter

Dieser internationalen Anmeldung liegen die nachstehend angekreuzten Unterlagen bei:

1. ☐	Unterzeichnete gesonderte Vollmacht	5. ☒	Blatt für die Gebührenberechnung
2. ☐	Kopie der allgemeinen Vollmacht	6. ☐	Gesonderte Angaben zu hinterlegten Mikroorganismen
3. ☐	Begründung für das Fehlen der Unterschrift	7. ☐	Sequenzprotokolle für Nucleotide und/oder Aminosäuren (Diskette)
4. ☒	Prioritätsbeleg(e) *(durch die Zeilennummer von Feld Nr. VI kennzeichnen).* (1)	8. ☐	Sonstige *(einzeln aufführen):*

Abbildung Nr. 1 der Zeichnungen (falls vorhanden) soll mit der Zusammenfassung veröffentlicht werden.

Feld Nr. IX UNTERSCHRIFT DES ANMELDERS ODER DES ANWALTS

Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht eindeutig aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.

Deutsche Telekom AG

i.A. .....

Eberhardt/Erkner, Patentabteilung,
EPA-Vollmacht Nr. 34337

☒ weitere Unterschriften werden nachgereicht

siehe Zusatzfeld Blatt 5

Vom Anmeldeamt auszufüllen

1. Datum des tatsächlichen Eingangs dieser internationalen Anmeldung:	2. Zeichnungen ☐ eingegangen: ☐ nicht eingegangen:
3. Geändertes Eingangsdatum aufgrund nachträglich jedoch fristgerecht eingegangener Unterlagen oder Zeichnungen zur Vervollständigung dieser internationalen Anmeldung:	
4. Datum des fristgerechten Eingangs der angeforderten Richtigstellungen nach Artikel 11(2) PCT	
5. Vom Anmelder benannte Internationale Recherchenbehörde: ISA/	6. ☐ Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchengebühr aufgeschoben

Vom Internationalen Büro auszufüllen.

Datum des Eingangs des Aktenexemplars beim Internationalen Büro:

Zusatzfeld ***Wird dieses Zusatzfeld nicht benutzt, so ist dieses Blatt dem Antrag nicht beizufügen.***

Dieses Feld ist in folgenden Fällen auszufüllen:

1. Wenn der Platz in einem Feld nicht für alle Angaben ausreicht:	***In diesem Fall sind mit dem Vermerk "Fortsetzung von Feld Nr..." [Nummer des Feldes angeben] die gleichen Angaben zu machen wie in dem Feld vorgesehen, das platzmäßig nicht ausreicht;***
insbesondere:	
i) Wenn mehr als zwei Anmelder und/oder Erfinder vorhanden sind und kein Fortsetzungsblatt zur Verfügung steht:	*In diesem Fall sind mit dem Vermerk "Fortsetzung von Feld Nr. III" für jede weitere Person die in Feld Nr. III vorgesehenen Angaben zu machen.*
ii) Wenn in Feld Nr. II oder III die Angabe "die im Zusatzfeld angegebenen Staaten" angekreuzt ist:	*In diesem Fall sind mit dem Vermerk "Fortsetzung von Feld Nr. II", "Fortsetzung von Feld Nr. III" oder "Fortsetzung von Feld Nr. II und Nr. III" die Namen der Anmelder und neben jedem Namen der Staat oder die Staaten (und/oder ggf. ARIPO-, europäisches oder OAPI-Patent) anzugeben, für die bezeichnete Person Anmelder ist.*
iii) Wenn der in Feld Nr. II oder III genannte Erfinder oder Erfinder/Anmelder nicht für alle Bestimmungsstaaten oder für die Vereinigten Staaten von Amerika als Erfinder benannt ist:	*In diesem Fall sind mit dem Vermerk "Fortsetzung von Feld Nr. II" oder "Fortsetzung von Feld Nr. III" oder "Fortsetzung von Feld Nr. II und Nr. III" der Name des Erfinders und neben jedem Namen der Staat oder die Staaten (und/oder ggf. ARIPO-, europäisches oder OAPI-Patent) anzugeben, für die bezeichnete Person Erfinder ist.*
iv) Wenn zusätzlich zu dem Anwalt/den Anwälten, die in Feld Nr. IV angegeben sind, weitere Anwälte bestellt sind:	*In diesem Fall sind mit dem Vermerk "Fortsetzung von Feld Nr. IV" für jeden weiteren Anwalt die gleichen Angaben zu machen wie in Feld Nr. IV vorgesehen.*
v) Wenn in Feld Nr. V bei einem Staat (oder bei OAPI) die Angabe "Zusatzpatent" oder "Zusatzzertifikat" oder wenn in Feld Nr. V bei den Vereinigten Staaten von Amerika die Angabe "Fortsetzung" oder "Teilfortsetzung" hinzugefügt wird:	*In diesem Fall sind mit dem Vermerk "Fortsetzung von Feld Nr. V" die Namen der betreffenden Staaten (oder OAPI) und nach dem Namen jeder dieser Staaten (oder OAPI) das Aktenzeichen des Hauptschutzrechts oder der Hauptschutzrechtsanmeldung und das Datum der Erteilung des Hauptschutzrechts oder der Einreichung der Hauptschutzrechtsanmeldung anzugeben.*
vi) Wenn die Priorität von mehr als drei früheren Anmeldungen beansprucht wird:	*In diesem Fall sind mit dem Vermerk "Fortsetzung von Feld Nr. VI" für jede weitere frühere Anmeldung die gleichen Angaben zu machen wie in Feld Nr. VI vorgesehen.*
2. Wenn der Anmelder für irgendein Bestimmungsamt die Vergünstigung nationaler Vorschriften betreffend unschädliche Offenbarung oder Ausnahmen von der Neuheitsschädlichkeit in Anspruch nimmt:	***In diesem Fall ist mit dem Vermerk "Erklärung betreffend unschädliche Offenbarung oder Ausnahmen von der Neuheitsschädlichkeit" nachstehend diese Erklärung abzugeben.***

Fortsetzung zu Feld Nr. IX
Unterschriften der Erfinder

.....

Dr. Alfred Scheerhorn

.....

Dr. Klaus Huber

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN** siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)	
P96029WO/EK03-3		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP97/05081	17/09/1997	01/10/1996
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK		
H04L9/32		
Anmelder		
DEUTSCHE TELEKOM AG et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 10 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☒ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
23/04/1998	23.02.99
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde: Europäisches Patentamt D-80298 München Tel. (+49-89) 2399-0 Tx: 523656 epmu d Fax: (+49-89) 2399-4465	Bevollmächtigter Bediensteter Nentwich, H Tel. Nr. (+49-89) 2399 8992

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP97/05081

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.)*:

Beschreibung, Seiten:

1,5,7,9	ursprüngliche Fassung			
2-4,6,8	eingegangen am	25/09/1998	mit Schreiben vom	22/09/1998

Patentansprüche, Nr.:

3,4,6,7,10	ursprüngliche Fassung			
1,2,5,8,9	eingegangen am	25/09/1998	mit Schreiben vom	22/09/1998

Zeichnungen, Blätter:

1/2,2/2	ursprüngliche Fassung

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:
   ☐ Ansprüche, Nr.:
   ☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-10
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	1-10
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-10
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen

siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

siehe Beiblatt

Zu Abschnitt V:

1 Stand der Technik

Die Erfindung bezieht sich auf ein Verfahren zum Übertragen von Signal-/Datenfolgen zwischen einem Sender und einem Empfänger mit Authentifizierung der übertragenen Signal-/Datenfolgen durch Verwendung von Schlüsseln und kryptographischen Algorithmen, die sowohl auf der Sender- als auch auf der Empfängerseite implementiert sind.

Bei der Übertragung von Signalfolgen spielt die authentische Übertragung der Daten bzw. Signale immer eine größere Rolle. So ist zum Beispiel in ISO/IEC 9797, Information technology - Security techniques - Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm (JTC1/SC27 1994) eine Lösung für dieses Problem beschrieben.

Diese Lösung hat jedoch den **Nachteil**, daß, um eine Änderung der Reihenfolge der übertragenen Daten zu erkennen, die Prüfsumme eines Signals abhängig von der Prüfsumme der bisher gesendeten Signale berechnet wird. Auch für den Fall, daß nach jedem Signal eine Prüfsumme gesendet wird, ist dies notwendig, da sonst ein Angreifer Signalprüfsummenpaare aufzeichnen und in geänderter Reihenfolge unbemerkt einspielen könnte. Dies erfordert in der bekannten Lösung für jede Prüfsumme eine Durchführung des kryptographischen Algorithmus. Da Reihenfolge und Auswahl der Signale nicht genau im voraus feststehen, ist es auch nicht möglich, die erforderlichen Prüfsummen im voraus zu berechnen. In einer zeitkritischen Umgebung kann dies zu Problemen führen.

2 Aufgabe, Lösung und deren Vorteile

Der Erfindung liegt deshalb die **Aufgabe** zugrunde, ein Verfahren zur authentischen Signal- bzw. Datenübertragung zu schaffen, das zu einem vorgegebenen Signalvorrat und einer vorgegebenen maximalen Anzahl zu übertragender Signale die Berechnung von Authentifikationsinformationen vorab ermöglicht, so daß in der Kommunikationsphase aus diesen schon vorher berechneten Informationen einfach und schnell Prüfsummen zu den gesendeten Signalen bzw. Daten berechnet werden können.

Die **Lösung** der Aufgabe besteht erfindungsgemäß darin, daß in einer Vorberechnungsphase mittels kryptographischer Algorithmen Daten abhängig von einem geheimen Schlüssel berechnet werden, aus denen in einer nachfolgenden Kommunikationsphase Authentifikationstoken für die Signale berechnet werden, die sowohl die Signale als auch die Reihenfolge des Sendens der Signale authentisieren.

Diese Lösung hat den **Vorteil**, daß es durch die bewußte Einführung einer Vorberechnungsphase und einer Kommunikationsphase in das Übertragungsverfahren jetzt möglich ist, die Berechnung von Authentifikationsinformationen schon vor der eigentlichen Kommunikationsphase durchzuführen. Während der Übertragungsphase können nun aus diesen schon vorher berechneten Informationen einfach und schnell Prüfsummen zu den gesendeten Signalen berechnet werden.

Das anmeldungsgemäße Konzept wird auch durch die im Internationalen Recherchenbericht genannten beiden Druckschriften der Kategorie A, die von dem Gegenstand des Anspruchs 1 weiter abliegen als der oben genannte Stand der Technik, weder offenbart noch nahegelegt.

Der Gegenstand des Anspruchs 1 ist offensichtlich auch gewerblich anwendbar.

Der vorliegende Anspruch 1 erfüllt somit die Erfordernisse gemäß Artikel 33(1) bis (4) PCT im Hinblick auf Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit.

Die Ansprüche 2 bis 10 sind von dem Anspruch 1 abhängig und können daher ebenfalls als neu, erfinderisch und gewerblich anwendbar angesehen werden.

Zu Abschnitt VII:

1 Auf der Seite 3 der Beschreibung wäre in der Zeile 7 "**werden**" durch "**wird**" zu ersetzen gewesen, da der Satz grammatikalisch richtig lauten müßte: "In der Vorberechnungsphase *wird ... eine Pseudozufallsfolge Z erzeugt.*"

2 In dem Anspruch 9 wäre "**nach dem Oberbegriff des Patentanspruchs 1 bzw.**" zu streichen gewesen. Da die Anmelderin mit dieser Streichung einverstanden war, hat sie diese wohl versehentlich nicht vorgenommen.

Auswahl der Signale nicht genau im Voraus feststehen, ist es auch nicht möglich, die erforderlichen Prüfsummen im Voraus zu berechnen.

In einer zeitkritischen Umgebung kann dies zu Problemen führen. Die Berechnung des kryptographischen Algorithmus kann zum Beispiel auf einer Chipkarte stattfinden. Beim Einsatz einer schon evaluierten Chipkarte ist dies vorteilhaft, ansonsten ist eine zusätzliche Softwareimplementierung des Algorithmus erneut zu evaluieren. Die Kommunikation mit der Chipkarte und die Berechnung des kryptographischen Algorithmus auf der Chipkarte sind sehr zeitintensiv.

Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren zur authentischen Signal- bzw. Datenübertragung zu schaffen, das zu einem vorgegebenen Signalvorrat und einer vorgegebenen maximalen Anzahl zu übertragender Signale die Berechnung von Authentifikationsinformationen vorab ermöglicht, so daß in der Kommunikationsphase aus diesen schon vorher berechneten Informationen einfach und schnell Prüfsummen zu den gesendeten Signalen bzw. Daten berechnet werden können.

Die erfindungsgemäße Lösung ist im Kennzeichen des Patentanspruchs 1 charakterisiert.

Weitere Lösungen der Aufgabe bzw. Ausgestaltungen des Erfindungsgegenstandes sind in den kennzeichnenden Teilen der Patentansprüche 2 bis 10 charakterisiert.

Durch die bewußte Einführung einer Vorberechnungsphase und einer Kommunikationsphase in das Übertragungsverfahren ist es jetzt möglich, die Berechnung von Authentifikations-informationen schon vor der eigentlichen Kommunikationsphase durchzuführen und während der Übertragungsphase können nun

aus diesen schon vorher berechneten Informationen einfach und schnell Prüfsummen zu den gesendeten Signalen berechnet werden. Die Lösung der Aufgabe besteht in einem Verfahren aus einer Vorberechnungsphase und einer Kommunikationsphase, in der die Signale bzw. Daten zusammen mit den Prüfsummen übertragen werden. In der Vorberechnungsphase werden mittels kryptographischer Algorithmen, zum Beispiel einer Blockchiffre im "Output-Feedback-Mode" aus dem Zeitvariantenparamenter (Sequenznummer, Zeitmarke und sonstigen Initialisierungsdaten) zunächst eine Pseudozufallsfolge Z erzeugt. Als Beispiel wird m = 16, 32 oder 64 für einen Sicherheitsparameter m angenommen. Aus der Folge Z werden jetzt sich nicht überschneidende Abschnitte z(i) von jeweils m Bit den Signalen s[i], i = 1, 2, ..., n des Signalvorrates zugeordnet. Aus der verbleibenden Folge werden weitere sich nicht überschneidende m Bit Abschnitte t[i] als Codierung der Nummern 1, 2, ... MAX gewählt, wobei MAX die maximale Anzahl der zu übertragenden Signale ist.

Wenn in der anschließenden Kommunikationsphase eine Senderauthentifikation erforderlich ist, wird zunächst dem Ablauf der "One pass authentication" gemäß den Veröffentlichungen ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication Mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994) und ISO/IEC 9798-4, Information technology - Security techniques - Entity authentication Mechanisms - Part 4: Mechanisms using a cryptographic check function (JTC1/SC27 1995) gefolgt. Der Sender überträgt die Initialisierungsinformation und die zeitvarianten Parameter an den Empfänger und als Authentisierungstoken sendet er eine Anzahl bisher nicht verwendeter Bits aus Z an den Empfänger. Der Empfänger berechnet seinerseits die Pseudozufallsfolge Z und überprüft das empfangene Authentisierungstoken. Die während der Signalübertragung

vom Empfänger empfangenen Signale werden als authentisch akzeptiert, wenn die empfangenen Authentifikationstoken mit denen, die er berechnet hat, übereinstimmen. Darüberhinaus sind noch Modifikationen des Verfahrens möglich, die in der nachfolgenden Beschreibung noch im Einzelnen beschrieben werden.

Die Erfindung wird nun anhand von in der Zeichnung dargestellten Ausführungsbeispielen näher beschrieben. In der Zeichnung bedeuten:

Fig. 1 ein Flußdiagramm für die prinzipielle Operationsfolge im Empfänger und

Fig. 2 ein Flußdiagramm für die prinzipielle Operationsfolge in einem Sender.

Das Verfahren besteht aus einer Vorberechnungsphase und einer Kommunikationsphase, in der die Signale zusammen mit den Prüfsummen übertragen werden.

Vorberechnungsphase:
Mittels des kryptographischen Algorithmus (zum Beispiel einer Blockchiffre im "Output-Feedback-Mode" gemäß ISO/IEC 10116, Information Processing - Modes of Operation for an n-bit Block Cipher Algorithm (JTC1/SC27 1991)) wird aus einem zeitvarianten Parameter (Sequenznummer, Zeitmarke, gemäß ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication Mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994)) und sonstigen Initialisierungsdaten zunächst eine Pseudozufallsfolge Z erzeugt. Es sei m ein Sicherheitsparameter, zum Beispiel M = 16, 32 oder 64. Aus der Folge Z werden jetzt sich nicht überschneidende Abschnitte z[i] von jeweils m Bits den Signalen s[i], i = 1, 2, ..., n des Signalvorrates zugeordnet. Aus der

die vom Sender empfangenen Authentifikationstoken mit denen, die er berechnet hat, übereinstimmen.

Die Reihenfolge der übertragenen Signale wird durch den Einfluß der Werte t[i] gesichert.

Eine Variante der Signalauthentifikation besteht im folgenden: Wenn es erforderlich ist, das Authentifikationstoken T(i) des i-ten Signals s[k[i-1]] abhängig von allen bisher gesendeten Signalen s[k[1]],...,s[k[i-1]] zu wählen, kann zur Authentifikation des i-ten Signals s[k[i]] das Token

$$T(i) = f(t[i], F(i)) \text{ gesendet werden, wobei}$$

$$F(1) = s[k[1]] \quad \text{und}$$

$$F(i) = f(s[k[i]],F(i-1)) \text{ für } i > 1.$$

Die Berechnung des Authentifikationstokens T(i) erfordert somit zweimal die Berechnung von f.

Ein Beispiel für die Anwendung eines derartigen Verfahrens ist der authentische Verbindungsaufbau beim Telefonieren. Beim Senden der Wahltöne ist nicht bekannt, ob noch ein weiterer Wahlton folgt. Deshalb erscheint es erforderlich, jeden Wahlton in der ihm nachfolgenden Pause durch die Übertragung eines Tokens zu authentisieren. Beim Mehrfrequenzwahlverfahren beträgt die Länge der Wahltöne mindestens 65ms und die Pausenlänge zwischen den Wahltönen mindestens 80ms. Für die Authentifikation, wie sie hier beschrieben ist, ist auch diese kurze Zeitdauer von 145ms ohne Probleme ausreichend.

Zunächst soll anhand des Flußdiagramms nach Fig. 1 die Operations- oder Schrittfolge des Empfängers beschrieben werden.

In dem Telefonbeispiel ist der Sender das Telefon, gegebenenfalls ausgestattet mit Kryptomodul und/oder

s[max] = Bit (smax-1)*m+1 bis Bit smax*m der Zufallsfolge PRS

t[1] = Bit smax*m+1 bis Bit (smax+1)*m der Zufallsfolge PRS

...

t[tmax] = Bit (smax+tmax-1)*m+1 bis Bit (smax+tmax)*m der Zufallsfolge PRS

Anhand von Fig. 2 wird nachfolgend die Operations- oder Schrittfolge für den Sender beschrieben.

S3: Der Sender wartet auf ein Signal w, das authentisch übertragen werden soll. w wird als natürliche Zahl zwischen 1, 2, ..., smax interpretiert, um die Abbildung w -> s[w] einfach zu halten.

S4: Der Sender sendet das i-te Signal w zusammen mit dem Authentifizierungstoken f(s[w],t[i]). Im Telefonbeispiel ist das Token f(s[w],t[i])=s[w]⊕t[i], das bitweise XOR von s[w] und t[i].

S5: S3 und S4 werden solange iteriert wiederholt, bis entweder keine Signale mehr authentisch übertragen werden sollen oder die maximale Anzahl von Signalen, die mit diesem Vorrat an vorberechneter Zufallsfolge PRS authentisiert werden können, erreicht ist.

S6: Im Telefonbeispiel wartet der Sender jetzt auf den Verbindungsaufbau des Empfängers.

E3, E4 und E5: Solange neue Signale mit zugehörigen Authentisierungstoken empfangen werden, prüft der Empfänger, ob die von ihm berechneten Authentisierungstoken mit den empfangenen übereinstimmen.

NEUER PATENTANSPRUCH 1

1. Verfahren zum Übertragen von Signal-/Datenfolgen zwischen einem Sender und einem Empfänger mit Authentifizierung der übertragenen Signal-/Datenfolgen durch Verwendung von Schlüsseln und kryptographischen Algorithmen, die sowohl auf der Sender- als auch auf der Empfängerseite implementiert sind, dadurch gekennzeichnet,

   daß in einer Vorberechnungsphase mittels kryptographischer Algorithmen Daten abhängig von einem geheimen Schlüssel berechnet werden, aus denen in einer nachfolgenden Kommunikationsphase Authentifikationstoken für die Signale berechnet werden, die sowohl die Signale als auch die Reihenfolge des Sendens der Signale authentisieren.

NEUER PATENTANSPRUCH 2

2. Verfahren nach Patentanspruch 1, dadurch gekennzeichnet,

daß in der Vorberechnungsphase mittels eines kryptographischen Algorithmus eine Pseudozufallsfolge (PRS) erzeugt wird,

daß aus dieser Folge bestimmte Abschnitte als Codierung sowohl der Signale eines Signalvorrates als auch der Sendestellen (1, 2, ... MAX) verwendet werden und

daß das Authentifikationstoken des Signals, das an i-ter (i = 1, 2, ..., MAX) Stelle gesendet wird, abhängig von der Codierung des Signals und von der Codierung der Sendestelle (i) berechnet wird.

NEUER PATENTANSPRUCH 5

5. Verfahren nach Patentanspruch 4, dadurch gekennzeichnet,

daß das Authentifikationstoken (T) des Signals, das an i-ter Stelle (i = 1, 2, ... MAX) gesendet wird, die bitweise XOR-Verknüpfung oder eine äquivalente logische Verknüpfung der Codierung aller bisher gesendeten Signale (1, 2, ... i) und der Codierung der Sendestelle (i) ist.

NEUER PATENTANSPRUCH 8

8. Verfahren nach Patentanspruch 2 oder 4, dadurch gekennzeichnet,

daß die Pseudozufallsfolge (PSR) durch Betreiben der Blockchiffre im bekannten "Output-Feedback-Mode" erzeugt wird.

NEUER PATENTANSPRUCH 9

9. Verfahren nach dem Oberbegriff des Patentanspruchs 1 bzw. nach einem der Patentansprüche 1 bis 8, dadurch gekennzeichnet,

daß in der Vorberechnungsphase zusätzlich ein Token (T) zur Authentifikation des jeweiligen Senders berechnet wird, das nachfolgend übertragen wird und den Empfänger zur Authentifikation des Senders initiiert.

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04L 9/32

A1

(11) Internationale Veröffentlichungsnummer: WO 98/15085

(43) Internationales Veröffentlichungsdatum: 9. April 1998 (09.04.98)

(21) Internationales Aktenzeichen: PCT/EP97/05081

(22) Internationales Anmeldedatum: 17. September 1997 (17.09.97)

(30) Prioritätsdaten:
196 40 526.2 1. Oktober 1996 (01.10.96) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELECOM AG [DE/DE]; Friedrich–Ebert–Allee 140, D–53113 Bonn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: SCHEERHORN, Alfred [DE/DE]; Ahornallee 3, D–49716 Meppen (DE). HUBER, Klaus [DE/DE]; Ernst–Ludwig–Strasse 21, D–64283 Darmstadt (DE).

(81) Bestimmungsstaaten: CA, IL, JP, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht

Mit internationalem Recherchenbericht.

Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.

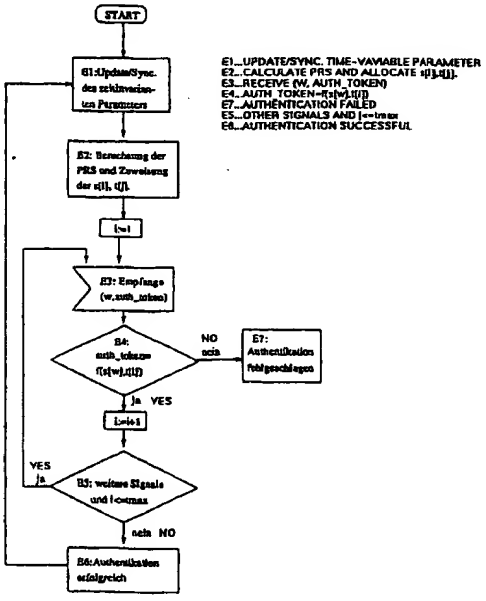
Kopie an Ref.

(54) Title: SIGNAL TRANSMISSION PROCESS

(54) Bezeichnung: VERFAHREN ZUR ÜBERTRAGUNG VON SIGNALEN

(57) Abstract

A process for transmitting sequences of signals/data from a transmitter to a receiver and for authenticating the sequences of signals/data consists of a precalculation phase and of a communication phase in which the signals are transmitted together with the checking sums. In the precalculation phase, a pseudo–random sequence is first generated by means of a cryptographic algorithm from a time–variable parameter and other initialisation data. Non–overlapping sections (z(1)) of a sequence (z) having each m bits are associated to signals (s(i)), wherein i = 1, 2, ... n, of a signal storage. Further non–overlapping m bit sections (t(i)) of the remaining sequence are selected for coding numbers (1, 2, ... MAX). The transmitter transmits the initialisation information and the time–variable parameters to the receiver and the receiver calculates the pseudo–random sequence (Z) and checks the received authentication token (T). The transmitter accepts the received signals as being authentic when the received authentication tokens match the calculated ones.



(57) Zusammenfassung

Das Verfahren zum Übertragen von Signal–/Datenfolgen von einem Sender zu einem Empfänger mit Authentifizierung der Signal–/Datenfolgen setzt sich aus einer Vorberechnungsphase und einer Kommunikationsphase zusammen, in der die Signale zusammen mit den Prüfsummen übertragen werden. In der Vorberechnungsphase wird mittels eines kryptographischen Algorithmus aus einem zeitvarianten Parameter und sonstigen Initialisierungsdaten zunächst eine Pseudozufallsfolge erzeugt. Aus einer Folge (z) werden sich nicht überschneidende Abschnitte (z(i)) von jeweils m Bits in Signalen (s(i)), i = 1, 2, ... n eines Signalvorrates zugeordnet. Aus der verbleibenden Folge werden weitere sich nicht überschneidende m Bit–Abschnitte (t(i)) als Codierung der Nummern (1, 2, ... MAX) gewählt. Der Sender überträgt die Initialisierungsinformation und die zeitvarianten Parameter an den Empfänger und der Empfänger berechnet seinerseits die Pseudozufallsfolge (Z) und prüft das empfangene Authentifikationstoken (T). Der Sender akzeptiert die empfangenen Signale als authentisch, wenn die vom Sender empfangenen Authentifikationstoken mit denen übereinstimmen, die er berechnet hat.

EL169614947US

Not entered
not part of translation

Translation of Revised German Page 3 of the Specification

...check sums for the signals transmitted can be calculated easily and quickly from this information previously calculated. The desired object is achieved by a method composed of a preliminary calculation phase and a communication phase in which the signals or data are transmitted together with the check sums. In the preliminary calculation phase, first a pseudo-random sequence Z is generated by cryptographic algorithms, e.g., a block cipher in the output feedback mode, from the time-variant parameter (sequence number, time mark and other initialization data). As an example, m = 16, 32 or 64 is assumed for a security parameter m. Then nonintersecting strings z(i) of m bits each from sequence Z are assigned to signals s[i], i = 1, 2, ..., n of the signal supply. Additional nonintersecting m-bit strings t[i] are selected from the remaining sequence as the coding of numbers 1, 2, ... MAX, where MAX is the maximum number of signals to be transmitted.

If transmitter authentication is necessary in the subsequent communication phase, then first the sequence of one pass authentication is performed according to the publications ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994) and ISO/IEC 9798-4, Information technology - Security techniques - Entity authentication mechanisms - Part 4: Mechanisms using a cryptographic check function (JTC1/SC27 1995). The transmitter transmits the initialization information and the time-variant parameters to the receiver, and it transmits a number of previously unused bits from Z to the receiver as an authentication token. The receiver in turn calculates pseudo-random sequence Z and checks the received authentication token. The signals received by the receiver during the signal transmission...

EL169614947US

New Patent Claim 9

9. Method according to one of Patent Claims 1 through 8, characterized in that a token (T) for authentication of the respective transmitter is also calculated in the preliminary calculation phase and is transmitted subsequently, initializing the receiver for authentication of the transmitter.

S:\NY3DOCS\TRL\PF01\68898-1-2345-62

Revised Page

Translation of New German Pages 2-4, 6 and 8 of the Specification

... selection of signals are not precisely fixed in advance, it is also impossible to calculate the required check sums in advance.

This can lead to problems in a time-critical environment. The cryptographic algorithm can be calculated on a chip card, for example. This is advantageous when using a chip card that has already been evaluated, because otherwise an additional software implementation of the algorithm must be evaluated again. Communication with the chip card and calculation of the cryptographic algorithm on the card are very time intensive.

Therefore, the object of the present invention is to create a method of authentic signal and data transmission that will permit calculation of authentication information with a given signal supply and a given maximum number of signals to be transmitted, so that check sums for the signals and/or data transmitted can be calculated quickly and easily from this previously calculated information in the communication phase.

The method of achieving this goal according to the present invention is presented in the characterizing part of Patent Claim 1.

Additional embodiments of the object of the present invention and methods of achieving this goal are presented in the characterizing parts of Patent Claims 2 through 10.

By intentionally introducing a preliminary calculation phase and a communication phase into the transmission process, it is now possible to perform the calculation of authentication information before the actual the transmission phase, and then during the transmission phase, check sums for the signals transmitted can be calculated easily and quickly from this information previously calculated. The desired object is

EL169614947US

implementation of the algorithm must be evaluated again. Communication with the chip card and calculation of the cryptographic algorithm on the card are very time intensive.

Therefore, the object of the present invention is to create a method of authentic signal and data transmission that will permit calculation of authentication information with a given signal supply and a given maximum number of signals to be transmitted, so that check sums for the signals and/or data transmitted can be calculated quickly and easily from this previously calculated information in the transmission phase.

The method of achieving this goal according to the present invention is presented in the characterizing part of Patent Claim 1.

Additional embodiments of the object of the present invention and methods of achieving this goal are presented in the characterizing parts of Patent Claims 2 through 10.

By intentionally introducing a preliminary calculation phase and a communication phase into the transmission process, it is now possible to perform the calculation of authentication information before the actual the transmission phase, and then during the transmission phase, check sums for the signals transmitted can be calculated easily and quickly from this information already calculated. The desired object is achieved by a method composed of a preliminary calculation phase and a communication phase in which the signals or data are transmitted together with the check sums. In the preliminary calculation phase, first a pseudo-random sequence Z is generated by cryptographic algorithms, e.g., a block cipher in the output feedback mode, from the time-variant parameter (sequence number, time mark and other initialization data). As an example, m = 16, 32 or 64 is assumed for a security parameter m. Then nonintersecting strings z(i) of m bits each from the sequence Z are assigned to the signals s[i], i = 1, 2, ..., n of the signal supply. Additional nonintersecting m-bit

strings t[i] are selected from the remaining sequence as the coding of the numbers 1, 2, ... MAX, where MAX is the maximum number of signals to be transmitted.

If transmitter authentication is necessary in the subsequent communication phase, then first the sequence of one pass authentication is followed according to the publications ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994) and ISO/IEC 9798-4, Information technology - Security techniques - Entity authentication mechanisms - Part 4: Mechanisms using a cryptographic check function (JTC1/SC27 1995). The transmitter transmits the initialization information and the time-variant parameters to the receiver, and it transmits a number of previously unused bits from Z to the receiver as an authentication token. The receiver in turn calculates pseudo-random sequence Z and checks the received authentication token. The signals received by the receiver during the signal transmission are accepted as authentic if the received authentication token matches the token calculated. In addition, modifications of the method are also possible, as described in detail in the following specification.

The present invention will now be described in greater detail on the basis of embodiments illustrated in the drawing, which shows:

Figure 1 a flow chart for the schematic operation sequence in the receiver, and

Figure 2 a flow chart for the schematic operation sequence in a transmitter.

This method includes a preliminary calculation phase and a communication phase in which the signals are transmitted together with the check sums.

Preparatory phase:

Using the cryptographic algorithm (for example, a block cipher in the output feedback mode according to ISO/IEC 10116, Information Processing - Modes of operation for an n-bit block cipher algorithm (JTC1/SC27 1991)), first a pseudo-random sequence Z is generated from a time-variant parameter (sequence number, time mark, according to ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994)) and other initialization data. Let m be a security parameter, such as M = 16, 32 or 64. Then from the sequence Z, nonintersecting strings z[i] with m bits each are assigned to signals s(i), i = 1, 2, ..., n of the signal supply. Additional nonintersecting m-bit strings t[i] are selected from the remaining sequence as the coding of numbers 1, 2, ... MAX, where MAX is the maximum number of signals to be transmitted.

Communication phase:

a) Transmitter authentication:

If transmitter authentication is necessary, first the sequence of one pass authentication is followed according to the publication ISO/IEC 9798-2, Information technology - Security techniques - Entity authentication mechanisms - Part 2: Mechanisms using symmetric encipherment algorithms (JTC1/SC27 1994), and ISO/IEC 9798-4 Information technology - Security techniques - Entity authentication mechanisms - Part 4: Mechanisms using a cryptographic check function (JTC1/SC27 1995). The transmitter transmits the initialization information and the time-variant parameters to the receiver. It transmits as the authentication token a number of previously unused bits from Z to the receiver. The receiver in turn calculates pseudo-random sequence Z and checks the received authentication token.

b) Signal transmission and authentication:

New Patent Claim 1

1. A method of transmitting signal/data sequences between a transmitter and a receiver with authentication of the transmitted signal/data sequences by using keys and cryptographic algorithms, which are implemented on the transmitter end as well as on the receiver end, characterized in that
in a preliminary calculation phase, data is calculated as a function of a secret key using cryptographic algorithms, and then in a subsequent communication phase, authentication tokens for the signals are calculated from this data, authenticating both the signals as well as the sequence in which the signals are transmitted.

New Patent Claim 2

2. The method according to Patent Claim 1, characterized in that
in the preliminary calculation phase, a pseudo-random sequence (PRS) is generated using a cryptographic algorithm;
certain strings from this sequence are used as a code for the signals of the signal supply as well as the transmitting stations (1, 2, ... MAX); and
the authentication token of the signal transmitted at the i-th position (i = 1, 2, ..., MAX) is calculated as a function of the coding of the signal and the coding of the transmission position (i).

New Patent Claim 5

5. The method according to Patent Claim 4, characterized in that the authentication token (T) of the signal transmitted at the i-th position (i = 1, 2, ..., MAX) is the bit-by-bit XOR link or an equivalent logic link of the coding of all previously transmitted signals (1, 2, ... i) and the coding of the transmission position (i).

New Patent Claim 8

8. The method according to one of Patent Claims 2 or 4, characterized in that the pseudo-random sequence (PRS) is generated by operating the block cipher in the known output feedback mode.

New Patent Claim 9

9. Method according to the definition of the species of Patent Claim 1 or according to one of Patent Claims 1 through 8, characterized in that a token (T) for authentication of the respective transmitter is also calculated in the preliminary calculation phase and is transmitted subsequently, initializing the receiver for authentication of the transmitter.

Let s[k[1]] be the first signal transmitted; then the transmitter transmits T(1): = f(z[k[1]], t[1]), where f is a link between the two values z[k[1]] and t[1] that can be calculated rapidly for authentication of the first signal. One example of f is the bit-by-bit XOR link.

For i = 2, 3, ..., i maximally MAX, let s[k[i]] be the i-th signal transmitted. For authentication of this signal, the transmitter transmits token T(i): = f(z[k[i]], t[i]). The receiver performs the same calculations and accepts the received signals as authentic if the authentication token received by the transmitter matches the token calculated.

The sequence of transmitted signals is guaranteed by the influence of the values t[i].

One variant of signal authentication proceeds as follows: If it is necessary to select authentication token T(i) of the i-th signal s[k[i-1]] as a function of all previously transmitted signals s[k[1]], ..., s[k[i-1]], then the token

T(i) = f(t[i], F(i)) can be transmitted for authentication of the i-th signal s[k[i]], where

F(1) = s[k[1]] and

F(i) = f(s[k[i]], F(i-1)) for i > 1.

Calculation of authentication token T(i) thus requires calculation of f twice.

One example of application of such a method is the authentic establishment of a connection in making a telephone call. When transmitting the dial tones, it is not known whether an additional dial tone will follow. Therefore, it seems necessary to authenticate each dial tone by transmitting a token in the pause following it. With multi-frequency dialing methods, the length of the dial tones is at least 65 ms, and the length of the pause between dial tones is at least 80 ms. With the authentication described here, this short interval of 145 ms for authentication is possible with no problem.